Chapter 2 Revisions - 2007

020103 Securing Unattended Work Stations

Purpose: To prevent unauthorized system access.

STANDARD

Workstations shall be safeguarded from unauthorized access—especially when left unattended. Each agency shall be responsible for configuring all workstations to require a password-protected screen saver after a maximum of thirty (30) minutes of inactivity. Users shall not disable the password-protected configuration specifications established by their agency.

GUIDELINE

When leaving workstations unattended, users should password protect them.

RELATED INFORMATION

Standard 050706 Log on and Log off from Your Computer

ISO 27002 REFERENCES
11.3.2 Unattended user equipment
11.3.3 Clear desk and clear screen policy

020106 Managing Passwords

Purpose: To prevent unauthorized access and to establish user accountability when using IDs and passwords to access State information systems.

STANDARD

Agencies shall manage passwords to ensure that all users are properly identified and authenticated before being allowed to access State information systems. The combination of a unique User ID and a valid password shall be the minimum requirement for granting access to an information system when IDs and passwords are selected as the method of performing identification and authentication. A unique user ID shall be assigned to each user so that individual accountability can be established for all system activities. Management approval shall be required for each user ID created. A process shall be in place to remove, suspend or reassign user IDs that become inactive as a result of employee or contractor movements. The system's authentication system shall limit unsuccessful logon attempts. Information shall be maintained on all logon attempts to facilitate intrusion detection. Password management capabilities and procedures shall be established to ensure secrecy of passwords and prevent exploitation of easily guessed passwords or weaknesses arising from long-life passwords. Each agency shall evaluate its business needs and the associated risks for its information systems in conjunction with identification and

authentication requirements. When IDs and passwords are selected as the method of performing identification and authentication, agencies are required to select and use the appropriate standards and best practices. Agencies must specify the minimum requirements for identification and authentication using IDs and passwords in accordance with the standard criteria that follow. Depending on the operating environment and associated exposures, additional or more stringent security practices may be required.

- For secured access to systems and applications that require a low level of security, passwords shall have at least six (6) characters of any sort.
- For access to all systems and applications that require a high level of security, such as electronic fund transfers, taxes and credit card transactions, passwords shall be at least eight (8) characters.
- To the extent possible, passwords shall be composed of a variety of letters, numbers and symbols[1] with no spaces in between.
- To the extent possible, passwords shall contain random characters from the required categories of letters, numbers and symbols.
- Passwords shall not contain dictionary words or abbreviations.
- Passwords shall not contain number or character substitutes to create dictionary words (e.g., *d33psl33p* for *deep sleep*[2]).

.....

Password Management Standards

- Except as specifically allowed by the security administrator, passwords shall not be revealed to anyone, including supervisors, family members or co-workers. In special cases where a user must divulge a password, such as for system support, the user shall immediately change the password after the purpose for revealing the password has been achieved.
- Users shall enter passwords manually, except for simplified/single sign-on systems that have been approved by the State CIO.
- No automated password input shall be allowed, except for simplified/single sign-on systems that have been approved by the State CIO.
- Passwords shall not be stored in clear text on hard drives, diskettes, or other electronic media. If stored, passwords shall be stored in encrypted format.
- Password Changes:

---

[1] For Resource Access Control Facility (RACF), valid symbols are @, $, #, and _, and the first character of a password must be a letter and the password must contain a number.

[2] Other examples of numbers/symbols for letters are *0* for *o*, *$* or *5* for *S*, *1* for *i*, and *1* for *l*, as in *capta1n k1rk* or *mr5pock*.

- ~~Individual user passwords~~ Government employees and government contactor passwords (e.g., email, Web and calendar) used to access systems and applications shall be changed at least every ninety (90) days. Passwords shall not be reused until six additional passwords have been created.

- Passwords for citizens and business users do not need to be changed periodically; the use of strong passwords and periodic password changes, however, is strongly encouraged ,

- Passwords shall not be inserted into email messages or other forms of electronic communication without proper encryption. Conveying a password in a telephone call is allowed when a positive identification has been established.
- ~~Where~~ When it is possible and practical, access to password-protected systems shall be timed out after an inactivity period of thirty (30) minutes or less or as required by law, if the inactivity period is shorter than thirty (30) minutes.
- Passwords shall not be displayed in clear text during the logon process or other processes. Where possible, applications that require clear-text authentication shall be converted to equivalents that can use encryption.[3]
- Passwords shall be changed whenever there is a chance that the password or the system could be compromised.

. . . .

[3] Encryption is defined in the Security Architecture Chapter, Standard 3, Use Cryptography Based on Open Standards.